L3 MATHÉMATIQUES, 2021–2022
THÉORIE DES GROUPES
CORRIGÉ DE L'EXAMEN DU 11 JANVIER 2022

PAUL LESCOT

Exercice I

(1) On a

$$|G| = 1805 = 5.361 = 5.19^2.$$

On sait que n_5 divise $\dfrac{|G|}{5} = \dfrac{1805}{5} = 361 = 19^2$, et $n_5 \equiv 1[5]$; on a donc $n_5 \in \{1, 361\}$. Les valeurs possibles de n_5 sont donc 1 et 361.

(2) Soient S et T deux sous–groupes de G d'ordre 5 ; alors $S \cap T \subsetneq S$, donc $S \cap T$ est un sous–groupe strict de S, d'où $S \cap T = \{e_G\}$.

Vu que $n_5 \neq 1$, on a, d'après (1), $n_5 = 361$. Soient $(S_j)_{1 \leq j \leq 361}$ les sous–groupes d'ordre 5 de G. On vient de voir que les $(S_j \setminus \{e_G\})_{1 \leq j \leq 361}$ sont deux à deux disjoints et de cardinal $5 - 1 = 4$. Soit alors

$$\mathcal{E} := \bigcup_{j=1}^{361} S_j \setminus \{e_G\});$$

il s'avère que $|\mathcal{E}| = 361.4 = 1444$.

Soit maintenant U un 19–sous–groupe de Sylow de G ($|U| = 19^2 = 361$); les éléments de U sont d'ordre divisant 19^2, donc n'appartiennent pas à $\mathcal{E}$, d'où

$$U \subset G \setminus \mathcal{E}.$$

Mais

$$|G \setminus \mathcal{E}| = |G| \setminus |\mathcal{E}| = 1805 - 1444 = 361 = |U|$$

et

$$U = G \setminus \mathcal{E}.$$

Il y a donc au plus un 13–sous–groupe de Sylow de G, donc exactement un.

(3) Si $n_5 = 1$, l'unique sous–groupe d'ordre 5 de G est distingué dans G.

Si $n_5 \neq 1$, il résulte de (2) que G contient un unique sous–groupe U d'ordre 361 ; mais alors U est distingué dans G.

Dans chaque cas, nous avons mis en évidence un sous–groupe distingué de G autre que $\{e_G\}$ et G : G n'est pas simple.

Exercice II

(1) Notons $\overline{r}$ la classe du rationnel $r \in \mathbf{Q}$ dans $G = \dfrac{\mathbf{Q}}{\mathbf{Z}}$.

Soit $g \in G$; alors $g = \overline{r}$ pour un $r \in \mathbf{Q}$. On peut écrire

$$r = \frac{a}{b}$$

avec $a \in \mathbf{Z}$ et $b \in \mathbf{N} \setminus \{0\}$.

Alors

$$\begin{aligned} bg &= \underbrace{g + ... + g}_{b \text{ termes}} \\ &= \underbrace{\overline{r} + ... + \overline{r}}_{b \text{ termes}} \\ &= \underbrace{\overline{r + ... + r}}_{b \text{ termes}} \\ &= \overline{br} \\ &= \overline{a} \\ &= \overline{0} \\ &\quad (\text{car } a \in \mathbf{Z}) \\ &= 0_{\frac{\mathbf{Q}}{\mathbf{Z}}}. \end{aligned}$$

On a donc $bx = 0_{\frac{\mathbf{Q}}{\mathbf{Z}}}$, donc g est d'ordre fini divisant b.

(2) On a

$$p^n 0_G = 0_G$$

donc

$$0_G \in G_{p,n}.$$

Soit $(x, y) \in G_{p,n}^2$; alors

$$p^n(x - y) = p^n x - p^n y = 0_G - 0_G = 0_G$$

d'où

$$x - y \in G_{p,n}\,;$$

$G_{p,n}$ est donc bien un sous–groupe de G.

Soit $x \in G_{p,n}$; écrivons $x = \overline{r}$ pour un $r \in \mathbf{Q}$. Alors

$$\overline{p^n r} = p^n \overline{r} = p^n x = 0_G = \overline{0}$$

donc $a := p^n r \in \mathbf{Z}$. Divisons a par p^n : $a = p^n q + s$ avec $0 \leq s \leq p^n - 1$. Alors

$$r = \frac{a}{p^n} = q + \frac{s}{p^n}$$

et

$$x = \overline{r} = \overline{\frac{s}{p^n}}.$$

Réciproquement, si $x = \overline{\dfrac{s}{p^n}} (0 \leq s \leq p^n - 1)$, alors $p^n x = \bar{s} = \bar{0}$ et $x \in G_{p,n}$.

Les $\overline{\dfrac{s}{p^n}} (0 \leq s \leq p^n - 1)$ sont deux à deux distincts car, si

$0 \leq k < l \leq p^n - 1$, alors $0 < l - k < p^n$ et p^n ne divise pas $l - k$, d'où $\overline{\frac{k}{p^n}} \neq \overline{\frac{l}{p^n}}$.

On a donc

$$G_{p,n} = \{\overline{\frac{s}{p^n}}(0 \leq s \leq p^n - 1)\}$$

et

$$|G_{p,n}| = p^n.$$

(3) Soit H un sous–groupe de G d'ordre p^n. Pour chaque $x \in H$, l'ordre $\omega(x)$ de x divise l'ordre $|H| = p^n$ de H, donc $p^n x = 0_G$, soit $x \in G_{p,n}$. On a donc $H \subset G_{p,n}$; mais

$$|H| = p^n = |G_{p,n}|$$

d'où $H = G_{p,n}$.

G_p est un groupe infini dénombrable dont chaque sous–groupe de type fini est un p–groupe fini cyclique. On l'appelle le **p–groupe de Prüfer**.

Exercice III

(1) On sait qu'existent dans D_{2m} deux éléments t d'ordre 2 et x d'ordre m tels que $D_{2m} =< t, x >$ et $txt^{-1} = x^{-1}$.

De même existent dans D_{2n} deux éléments u d'ordre 2 et y d'ordre n tels que $D_{2n} =< u, y >$ et $uyu^{-1} = y^{-1}$.

Soient $a := (t, u) \in G$ et $b = (x, y) \in G$. Pour chaque $k \in \mathbf{Z}$, on a

$$b^k = (x^k, y^k),$$

donc $b^k = e_G$ si et seulement si $x^k = e_{D_{2m}}$ et $y^k = e_{D_{2n}}$, soit $\omega(x) \mid k$ et $\omega(y) \mid k$, ou $m \mid k$ et $n \mid k$. Vu que m et n sont premiers entre eux, cela revient à $mn \mid k$: on a donc $\omega(b) = mn$.

On voit (encore plus) facilement que a est d'ordre 2.

De plus

$$\begin{aligned} aba^{-1} &= (t,u)(x,y)(t,u)^{-1} \\ &= (t,u)(x,y)(t^{-1},u^{-1}) \\ &= (txt^{-1}, uyu^{-1}) \\ &= (x^{-1}, y^{-1}) \\ &= (x,y)^{-1} \\ &= b^{-1}. \end{aligned}$$

Il s'ensuit que le sous–groupe $< a, b >$ de G engendré par a et b est diédral d'ordre $2mn$: $H :=< a, b >$ convient.

(2) L'ordre de G est

$$|G| = |D_{2m} \times D_{2n}| = |D_{2m}|.|D_{2n}| = (2m)(2n) = 4mn.$$

L'indice de H dans G est donc

$$\begin{aligned}[G:H] &= \frac{|G|}{|H|}\\ &= \frac{4mn}{2mn}\\ &= 2.\end{aligned}$$

Il en résulte que H est d'indice 2 dans G ; il est donc distingué.

Exercice IV

(1) L'ordre de G est égal au nombre de quadruplets $(a,b,c,d) \in \mathbf{F}_p^4$ tels que $ad-bc \neq \bar{0}$. Si $a = \bar{0}$, cela revient à $bc \neq \bar{0}$, soit $b \neq \bar{0}$ et $c \neq \bar{0}$; on peut donc choisir d arbitrairement dans $\mathbf{F}_p$ et b et c dans $\mathbf{F}_p \setminus \{\bar{0}\}$.

Si $a \neq \bar{0}$, on peut choisir arbitrairement b et c dans $\mathbf{F}_p$, et reste alors une condition sur d : $d \neq \dfrac{bc}{a}$, d'où $p-1$ possibilités pour d.

On trouve donc

$$\begin{aligned}|GL_2(\mathbf{F}_p)| &= p(p-1)^2 + (p-1)p^2(p-1)\\ &= p(p-1)^2(p+1)\\ &= (p-1)(p+1)p(p-1)\\ &= (p^2-1)(p^2-p).\end{aligned}$$

(2) Soit $(M,N) \in G^2$; écrivons

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

et

$$N = \begin{bmatrix} e & f \\ g & h \end{bmatrix}.$$

Alors

$$MN = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

et

$$\begin{aligned}\det(MN) &= (ae+bg)(cf+dh) - (af+bh)(ce+dg)\\ &= (aecf + aedh + bgcf + bgdh) - (afce + afdg + bhce + bhdg)\\ &= aedh + bgcf - afdg - bhce\\ &= (ad-bc)(eh-gf)\\ &= \det(MN) :\end{aligned}$$

det est un morphisme de groupes.

Soit $x \in \mathbf{F}_p^*$; définissons

$$A := \begin{bmatrix} x & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}$$

Alors $A \in G$ et

$$\det(A) = x.\bar{1} - \bar{0}.\bar{0} = x :$$

det est surjectif.

(3) On a

$$\begin{aligned} \frac{G}{SL_2(\mathbf{F}_p)} &= \frac{G}{\ker(\det)} \\ &\simeq \mathrm{Im}(\det) \\ &= \mathbf{F}_p^* \end{aligned}$$

(car det est surjectif d'après (2)), d'où

$$\begin{aligned} \frac{p(p-1)^2(p+1)}{|SL_2(\mathbf{F}_p)|} &= \frac{|G|}{|SL_2(\mathbf{F}_p)|} \\ &= |\frac{G}{SL_2(\mathbf{F}_p)}| \\ &= |\mathbf{F}_p^*| \\ &= p-1, \end{aligned}$$

d'où

$$|SL_2(\mathbf{F}_p)| = p(p-1)(p+1).$$

(4) D'après (1), $GL_2(\mathbf{F}_2)$ est d'ordre $(2^2-1)(2^2-2) = 3.2 = 6$. Soient

$$A = \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \in GL_2(\mathbf{F}_2)$$

et

$$B = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix} \in GL_2(\mathbf{F}_2).$$

Alors

$$AB = \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}$$

et

$$BA = \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix},$$

d'où $AB \neq BA$.

Donc $GL_2(\mathbf{F}_2)$ est un groupe non abélien d'ordre 6 ; il est donc isomorphe à Σ_3.

On peut aussi remarquer que $GL_2(\mathbf{F}_2)$ agit naturellement sur $\mathbf{F}_2^2 \setminus \{\bar{0}, \bar{0}\}$, lequel est de cardinal 3 ; on obtient ainsi un morphisme de $GL_2(\mathbf{F}_2)$ dans Σ_3, dont l'on peut voir qu'il est bijectif.

(5) (**bonus**)

Soit

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(SL_2(\mathbf{F}_3)).$$

Alors M commute avec

$$\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}$$

et avec

$$\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix}$$

d'où

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

et

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

On a donc $a+b=a$, $c+d=a+c$ et $a=a+c$, soit $a=d$ et $b=c=\bar{0}$, d'où

$$M = \begin{bmatrix} a & \bar{0} \\ \bar{0} & a \end{bmatrix}.$$

Du fait que $M \in SL_2(\mathbf{F}_3)$, on a $a^2 = \bar{1}$ et $a \in \{\bar{1}, -\bar{1}\}$. Donc

$$Z(SL_2(\mathbf{F}_3)) \subset \{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} -\bar{1} & \bar{0} \\ \bar{0} & -\bar{1} \end{bmatrix} \}.$$

L'inclusion réciproque est évidente ; on a donc

$$Z(SL_2(\mathbf{F}_3)) = \{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} -\bar{1} & \bar{0} \\ \bar{0} & -\bar{1} \end{bmatrix} \}.$$

Mais alors

$$\begin{aligned} |\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}| &= \frac{|SL_2(\mathbf{F}_3)|}{|Z(SL_2(\mathbf{F}_3))|} \\ &= \frac{3(3-1)(3+1)}{2} \\ &\quad \text{(d'après (3))} \\ &= \frac{24}{2} \\ &= 12. \end{aligned}$$

Soit maintenant u la classe de

$$\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & -\bar{1} \end{bmatrix} \in SL_2(\mathbf{F}_3)$$

dans $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$, et soit v la classe de

$$\begin{bmatrix} \bar{0} & \bar{1} \\ -\bar{1} & \bar{0} \end{bmatrix} \in SL_2(\mathbf{F}_3)$$

dans $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$.

On voit aisément que u et v sont d'ordre 2, et que $uv = vu \neq 1_{\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}}$; $< u, v >$ est donc un sous–groupe de $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$ isomorphe au groupe de Klein. $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$ est donc un groupe d'ordre 12 dont un 2–sous–groupe de Sylow est isomorphe au groupe de Klein ; en vertu de la classification

des groupes d'ordre 12, il est donc soit isomorphe à $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{6\mathbf{Z}}$, soit diédral, soit isomorphe à $\mathcal{A}_4$.

Si l'on se trouvait dans l'un des deux premiers cas, $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$ aurait un unique sous–groupe d'ordre 3. Mais les classes dans $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$ de

$$\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix}$$

et de

$$\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}$$

engendrent deux sous–groupes distincts d'ordre 3, une contradiction. On a donc nécessairement

$$\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))} \simeq \mathcal{A}_4.$$

On peut aussi raisonner plus géométriquement : $SL_2(\mathbf{F}_3)$ agit naturellement sur l'ensemble des droites vectorielles de $\mathbf{F}_3^2$, lequel est de cardinal 4. On voit aisément que le noyau de cette action est $Z(SL_2(\mathbf{F}_3))$; on en déduit l'existence d'un plongement de $\frac{SL_2(\mathbf{F}_3)}{Z(SL_2(\mathbf{F}_3))}$ dans Σ_4. L'image de ce plongement est un sous–groupe d'ordre 12 de Σ_4 ; il s'agit donc de $\mathcal{A}_4$, d'où le résultat.